CA2ON
Z 3
-77E100

Government
Publications

Ontario

ELECTRONIC FUNDS TRANSFER
STUDY PROJECT

31761 11849464 0

The Challenge of EFT: Policy and Legislative Responses

December
1978

CA2ON
Z3
-77E100

THE CHALLENGE OF EFT

POLICY AND LEGISLATIVE RESPONSES TO ELECTRONIC FUNDS TRANSFER

LIBRARY
FEB
14
1979
UNIVERSITY

REPORT TO THE PROVINCE OF ONTARIO ON POLICY AND LEGISLATIVE RESPONSES TO ELECTRONIC FUNDS TRANSFER IN CANADA

Digitized by the Internet Archive
in 2024 with funding from
University of Toronto

https://archive.org/details/31761118494640

The Honourable R. Roy McMurtry, Q.C.
Attorney General
Queen's Park
Toronto, Ontario

Dear Mr. Attorney:

I have the honour of submitting to you and to your colleagues, the Honourable James W. Snow, Minister of Transportation and Communications and the Honourable Frank Drea, Minister of Consumer and Commercial Relations, my Report on policy and legislative responses to electronic funds transfer.

Richard H. McLaren
Project Director

December, 1978

This report is a summary of a research project funded by the Province of Ontario and directed by Professor Richard H. McLaren of the Faculty of Law at the University of Western Ontario. The eight background working papers of the project are the source from which the content of this report has been drawn.

PREFACE

It has been a privilege to direct the development of this unique piece of research. To the best of my knowledge this is the first Canadian research project to have been published dealing with the policy and legislative responses to electronic funds transfer in Canada. I would like to thank the Province of Ontario for giving me the opportunity to direct this project and to congratulate it in showing the initiative to have undertaken it.

The project could not have been brought to its successful conclusion without the dedicated assistance of my full-time research assistant Michael Fredericks, B.A., LL.B. His dedication, hard work and insightful assistance made the project the success it has been. I would also like to extend my thanks to my research students Miss Susan Ditta and Messrs. Pat Moran, Paul Stacey and Peter Johnson, all of whom made contributions to the work of the project.

There are a number of other people who made invaluable contributions to this project. Their assistance is what made this whole project interesting and worthwhile. I am indebted to all these people and would like to extend my thanks to them; the principal researchers who developed working papers; to Jean Carter, my secretary for her cheerful and willing assistance; to Miss Olive Donaldson, the secretary to the project; to Professors Bruce Welling, Earl Palmer and David Johnston for their very helpful comments and suggestions on early drafts of this report; to Mr. Gordon Donaldson for his very able assistance in revising the final report. Finally, I would like to thank the University of Western Ontario and the Faculty of Law for enabling me to carry out this project.

Richard H. McLaren
London, Ontario

November, 1978.

CONTENTS

THE CHALLENGE OF EFT

SECTION ONE: INVISIBLE MONEY

The Elizabethan thinker Francis Bacon said money was like muck, "no good except it be spread". Since his day, the shape of money has changed from gold coins and promissory notes to include imprints from plastic cards and invisible patterns on magnetic tape and the "spreading" is about to become instantaneous, as money changes hands between computer terminals connected by wire, microwave circuits or beams bounced across the oceans by satellites in space. Electronic Funds Transfer (EFT) systems, the next stage in computerized financial services, will handle much of the monetary muck-spreading in Canada within three to five years. A person's signature, the fundamental pledge on which our legal system is based, may be replaced by that individual's PIN (Personal Identification Number). Written records of transactions will become electronic impulses and, to an increasing extent, computers will replace human money changers. This revolution is already under way, and there are no laws adequate to cope with it.

The advantages of EFT to banks and near-banks (trust companies, caisses populaires, credit unions, etc.) are obvious -- increased speed and efficiency. If these result in lower bank charges, and greater convenience, the customer will gain, too. But EFT, by taking our already-computerized

money system a stage further into the electronic future, poses new threats to the customer's privacy, security from deliberate theft, and accidental loss through the muddles and mistakes which are all too frequent in computerized operations. It may turn him into a small, shaky digit, quivering before a colossal, unfeeling machine.

EFT is not here yet; it is not yet being used to any great extent even in the United States, home of the computer. But it is coming, and our present laws, provincial and federal, do not provide for adequate control or supervision of this important development. We do not even have laws governing credit cards, which have been widely used for ten years. Technology is often ahead of the law, but seldom so far ahead.

So in October, 1977, the Province of Ontario commissioned this research project to examine the state of EFT and propose policies and legislation to deal with it within the Province. The federal government is also studying it and it was hoped to include in this report an examination of Ottawa's proposals. But publication of federal reports has been postponed repeatedly,* so this study deals exclusively with matters within the provincial areas of jurisdiction.

At first glance, EFT seems to be a banking and telecommunications matter -- and banking and telecommunications are regulated by the federal government -- but on closer examination it becomes a question of individual privacy, consumer protection

* The final report of the Canadian Payments Systems Standards Group was published by the Department of Finance on December 15, 1978, as this report was going to press.

and responsibility in business transactions, which should be resolved by the Province, with or without federal initiative.

This report and its supporting working papers* comprise the first comprehensive Canadian study of the possible impact on provincial legislation of EFT developments. The sheer size and speed of these developments will probably make it, or any other study, obsolete within a few years. So the project was designed to be built upon by further government or private studies, and this report was designed to stimulate public debate. A definitive solution is not offered, but action is recommended now to bring the immediate problems posed by EFT under control.

These are set out in the following sections and explained in detail in four working papers: "Privacy, Confidentiality, and Security in a Canadian Electronic Funds Transfer System", "Electronic Funds Transfer and the British North America Act", "Proof of Payment and Evidentiary Problems", and "Transaction Cards in Canada". Each of these papers analyzes policy and legislative responses to the potential legal and social problems arising from EFT and all of them, except the constitutional paper, make specific recommendations on legislation. Those recommendations are set out in Section Eight of this report.

* A complete list of working papers for this project appears as an appendix to this report.

The following is a summary of the most important principles and recommendations of this report and its working papers:

1) EFT brings with it the well-known potential danger, inherent in the use of automated data processing technology, for breach of confidentiality of personal financial information. Ontario needs a financial privacy law which would prevent unauthorized third parties from gaining access to data on financial transactions. This initiative would cover credit card information, which is not yet under control, and would prevent abuses under EFT systems which will employ "Transaction Cards" and increase significantly the amount of computer-stored information on a citizen's finances.

2) EFT introduces, as well, the potential for "electronic theft" -- the stealing of money from computerized accounts by manipulation of computer systems. The law should provide that the system's owners be responsible for losses incurred, except where the customer's carelessness has made it possible for the theft to occur.

3) EFT will tend to supplant the existing "paper-based" system of effecting commercial transactions. The existing law and the time-tested techniques applicable to resolution of disputes in this area of activity, e.g., making proof of payment by exhibiting a cancelled cheque, will be rendered increasingly inadequate. At present, disputes over

computerized transactions often end in stalemate because the expense of retrieving the relevant information from the innards of the system is greater than the amount in dispute. The owner of the system should be obliged to absorb the cost of retrieving evidence from the system. Should a dispute reach the litigation stage, the existing laws of evidence appear to be inadequate to permit introduction as evidence in the proceedings, printouts of computerized data. The Ontario Evidence Act should be updated to take account of the fact that records of commercial transaction, the evidence required to resolve such disputes, are stored electronically, and not in written form.

4) EFT will tend to erode other practical advantages and protections inherent in the "paper-based" system. Thus, for example, one can stop payment on a cheque if the goods or services for which payment was made by cheque turn out to be faulty. It is then up to the receiver of the cheque to sue for payment. With EFT, the money changes hands instantaneously and the shoe is on the other foot. The customer should have the right to reverse an EFT transaction, even after payment is made. He must be able to hold liable the credit grantor who profits by a credit transaction, if the goods received by the customer are no good.

5) The introduction of EFT into the business life of the community and its future growth in importance is, perhaps unavoidably, an insidious process. The public has never been particularly interested in the workings of its financial institutions, so long as these worked reasonably smoothly, and the financial community, secretive by nature, has never rushed to bare its soul or explain its methods. So EFT is creeping upon us, stage by stage. Tellers' computer terminals, cash dispensers which require debit cards and identification numbers, payroll deposits on tape, coded symbols on products, are all forerunners of the complete EFT system. The considerable power of the banks and near-banks to coerce customers into using the system they prefer, may be used to push people into using EFT whether they like it or not. The system won't be economical unless it is universal, so we can expect considerable pressure to join. Consumers should be permitted to opt out. On the other hand, if EFT is going to save the consumer money, ways should be found for low-income groups, the people the financial houses don't really want as customers, to opt in.

These principles among others are spelled out in the body of this report and in the working papers. They should be the groundwork for a policy to deal with the problems of the EFT age which will soon be upon us.

SECTION TWO: THE GROWTH OF EFT

The ultimate goal of EFT systems is a fully automated and computerized flow of money in all its forms and in several directions -- between cash register and teller's cage, borrower and lender, payer and payee. The money will flow back and forth at lightning speed.

Complete EFT may not come for several decades, if ever, but the technology exists and some of the systems are already in place, like sections of a railway waiting to be linked together. Essentially, EFT is the replacement of written transactions. The cheque or the carefully signed and witnessed document is replaced by payments and promises to pay recorded on computer tapes, flashed fleetingly on screens or rattled out on automated printers.

EFT is growing out of the cheque payment system, just as cheques grew out of currency, which in turn grew out of the barter system. When the Canadian chartered banks found that the volume of paper cheques they had to process by hand was more than their system could handle, they introduced mechanized processing, based on machines that could recognize and read symbols on cheques faster than any human. At the time, they did not analyze and revamp the payments system as a whole to handle future business needs.

Gradually, during the 1960s, they examined automated banking techniques and discovered "on-line" banking in which

a number of computer terminals would be installed in a branch and hooked up to a central computer which processed and stored information formerly contained on ledger cards stored at the branch.

"On-line" banking developed in the 1970s -- the first major step toward EFT. It brought with it a fundamental change in banking philosophy, not only by the banks, but also by the near-banks which are traditionally less hidebound in their outlook and, therefore, quicker to adopt new systems. Bankers and near-bankers realized that they were no longer just intermediaries in financial transactions; they had become the prime processors and storers of information on which financial life depended. Automation created a sudden storehouse of electronic information which the banks could never have gathered while spending their employees' time processing ledger cards by hand. Because they had been excluded from the wider Canadian payments system, the near-banks saw the advantage of these early EFT developments and were the first to embrace them.

The early seventies brought bank credit cards as well as "on-line" banking. Chargex (now Visa/Chargex) went national in 1971 and Master Charge entered the field as its major competitor in 1973. The credit card process clogged the banks with even more paper than the cheque system, bringing more calls for more computers until the movement of paper was reduced and "descriptive billing" began. This was another EFT system, separate from the standard interbank clearing system

in which banks process one another's cheques and figure out who owes how much to whom.

The next development will probably be central credit card centres, beginning with a single Visa centre which will take over from the individual Visa/Chargex centres now operated by the banks participating in that credit card system. The central computer will update through instant connection with the present bank centres. As soon as a transaction occurs, the central computer will digest it. The chartered banks can then continue to operate as independent licensees of Visa/Chargex without keeping their own verification and payment records. This will mark another step towards centralization, and place records of payment that much farther away from the people who bought or sold.

Public acceptance of credit cards -- "plastic money" -- convinced the banks and near-banks that the public was ready for automatic cash dispensers and the more sophisticated automatic teller machines which not only give out money but take it in, credit it and even pay bills. At present the chartered banks are undecided whether to connect these EFT systems to their computerized banking or their credit card networks, but some form of transaction card will be needed to operate them. Again, the near-banks are ahead. One trust company has already contracted for 100 automatic teller machines. Such automation is likely to produce more and more branches of near-banks handling electronic money.

The first deposit clearing facility using magnetic tape to record transactions was introduced in Canada in 1976. It is the forerunner of a more efficient EFT system of the future. Already it is competing with the cheque system. No cheques need be produced; taped instructions to credit the payees' accounts are all that is needed. The tape is processed electronically by the bank or near-bank. Large corporations and governments now use taped credit transfers extensively. The system is now used to make regular deposits, including interest on the current issue of Canada Savings Bonds and could be used to debit consumers' bank accounts to pay their gas, hydro and telephone bills. Magnetic bills have not yet come to Canada but are likely to arrive within a few years. The importance of the cheque is being eroded by EFT.

Point of sale terminals (POS) which will "bleep" your supermarket bill straight to your bank as soon as you make your purchase, and instantly take the money out of your account, are not yet in use in Canada. But the groundwork has been laid and the symbols -- the universal product code on most supermarket products -- are there, ready to be read by electronic scanners and form part of the system. A transaction card would be used to trigger an almost instantaneous transfer of funds from the customer's account to that of the supermarket or other store, via the bank. With the present credit card systems, transactions are based, ultimately, on paper bills and signatures on paper. Only information about the customer's credit rating and reliability is stored electronically. With the POS system

the payment itself would be made electronically and the paper kept only for record, if it is kept at all.

The POS terminal, plus the automatic teller machine is a revolutionary combination. It would work either to credit or debit the customer's account. The same card could be used to pay for goods or services by drawing on the customer's line of credit (the credit mode) or by drawing on his bank account (the debit mode). When this system is extended to large-scale commercial and industrial transactions -- when millions of dollars are transmitted at the flip of a key -- EFT will have arrived and reached what now appears to be its objective. No one can predict where it may go from there.

SECTION THREE: PRIVACY IN DANGER

EFT will be a centralized, computerized operation and, as such, a threat to personal privacy. Any operation which takes a vast body of information, collates and stores it so that it becomes instantly retrievable by any authorized person -- and possibly by unauthorized persons who have found a key to the electronic safe -- poses a challenge to privacy.

The right to privacy is something all of us think we have, but in fact, do not have. There has never been adequate legal recognition of the right to privacy in Canada. Privacy is, in very general terms, the desire to be left alone and to control the dissemination of information about oneself. All that exists now is the notion of confidentiality, based on English common law of the mid-19th century. It requires that banks not disclose information about a customer to a third party because of an implied contract between the banker and his customer. The bank can, of course, disclose this information with the customer's consent. This is frequently obtained when the customer opens an account by getting him to sign a standard contract form containing a blanket consent.

Apart from this principle of common law there are few federal and Ontario statutory controls on the disclosure of financial information. There are no provisions for confidentiality in the federal Bank Act or the Ontario Loan and Trust Companies Act, although there is a provision in the recent

Ontario Credit Unions and Caisses Populaires Act (Subsections 75(1) and (3)).

Both the Ontario and Canada Evidence Acts contain provisions regulating the legal right to compel disclosure of financial information and the Ontario Consumer Reporting Act also provides a certain amount of confidentiality but, by and large, there is little protection of a person's privacy. Yet demand for such protection is growing. Technological change has eroded the individual's ability to protect his own privacy. There is a growing feeling in the United States and Canada that the law has to step in to set a balance between individual and public interests in financial matters; between computerized efficiency and human dignity.

The "right to privacy" is an illusion in the legal sense for there is no such right. Perhaps, in the past, there has been no real need for it. But EFT and other developments are forcing upon our society the need for some form of protection of the individual from the computer. EFT is only a part, but an important one, of the problem of privacy within the Province of Ontario. Privacy, as will be argued in the constitutional section of this report (Section Six) is a matter for the Legislature of this Province to define and protect.

It is not necessary to establish the legitimacy of the claim to privacy, confidentiality, and security from improper use of financial information. It should be enough to note that Canadians have come to expect this; so a way must be found to

establish it, in the face of EFT and future unknown threats to privacy which may lurk beyond.

The right of privacy, within the province, can best be established through a combination of legislation and self-regulation. There must be co-operation between government and those industries most likely to impinge upon person privacy.

Law enforcement agencies impinge on personal privacy in order to do their jobs, and their needs must be taken into consideration. So must legitimate needs for access to financial information by other government bodies and financial institutions. Legislators, with the ultimate assistance of the courts, must strike the balance between the public's interest in financial records and the individual's interest in keeping his financial affairs to himself.

The dissemination of EFT data must be controlled. Through their vital power to grant or withhold credit, financial institutions can demand from the borrower a blanket waiver of confidentiality. If, having read the fine print, the borrower gives his informed consent, it may be legitimate; but he should not be forced to submit to unnecessary loss of privacy in order to borrow or deposit money.

One of the most disturbing facts established by the research for this project is that customers DO give up their right to confidentiality by signing waiver clauses. If these waiver clauses were prohibited by law, the financial institutions

would have greater respect for confidentiality and privacy and be more concerned with the rights, legal and otherwise, of their customers.

The research for this project found the common law approach inadequate to deal with either confidentiality or privacy. The principle of confidentiality is not sufficiently well-developed and is easily avoided by appropriate contractual language; the right of privacy is non-existent. It is difficult to impress upon new bank employees the importance of confidentiality or the difference between handing out information on a person's bank loans and his bank deposits. Loan information may, under certain circumstances, be passed on to third parties to help establish credit ratings. But the size of a customer's bank account is a private matter between the customer and the bank.

(3.1) *It is recommended that Ontario enact a statutory right to financial privacy. This legislation would establish who has the right of access to financial data and limit the use of disclosed information to such authorized persons. These persons would be permitted to use the data only for the purposes for which access was granted. Failure to observe such standards would give rise to statutory rights to damages against the financial institution concerned. This legislation could be part of a broader piece of legislation dealing with privacy.*

(3.2) *It is recommended further that financial institutions improve their methods of handling personal information relating to their customers, in order to ensure the highest standards of confidentiality. The government should monitor their progress and, if self-regulation fails, enact legislation to protect the confidentiality of customer data and information about financial transactions by setting rules for proper employee conduct.*

Banks take great pains to guard the money locked up in their vaults. Guarding computerized financial information, which is another form of money just as valuable as bullion, is much more difficult. For computer systems are vulnerable to unauthorized access and no security measures provide absolute protection against tampering by outsiders.

There are at least four potential security problems in EFT systems: the use of a stolen access card and the PIN identification number that goes with it to activate a remote computer terminal; access to the central store of data by employees at remote terminals; access by employees or outsiders at the central processing unit itself; and wire-tapping of communication lines.

Stolen cards are dealt with in a later section. The following is a review of the better security measures now being taken by financial institutions. As stated above, none of these provide absolute security.

The principle that no operator of a computerized data system should have access to the entire system is one safeguard. Each operator should have a coded "password" to activate his part of the system. Printed summaries of all transactions should be provided by all the computer terminals along the line, from the point at which a transaction begins to the branch office which may handle it and then to the data centre. By constantly comparing and auditing this information, the risk of dishonest data being fed into the system or data dishonestly retrieved, is reduced. This also discourages "fishing expeditions" by persons searching for information to which they are not entitled.

In the data centre itself, the responsibilities of the staff should be divided among product managers, systems analysts and programmers, so that no group controls everything. The system development personnel should be kept apart from the operators.

Information is now being transmitted from remote terminals to the data centres by Bell Canada telephone wires -- in most cases without being put into code. Thus, an enterprising wiretapper is able to intercept information, understand it, and use it. This information should not only be coded, but limited, so that if it is intercepted no important personal data will be revealed.

(3.3) *It is recommended that an industry-government committee be established to draw up guidelines for the confidentiality and security of customer data and financial transaction information. These should include measures to restrict unauthorized access to data by employees of financial institutions, division of responsibilities among employees and monitoring of the systems. Special training programs for employees should be established.*

SECTION FOUR: PAYING BY NUMBERS

The transaction card, which will be the key to the automated world of EFT, is a development of the credit card. It is a super-credit card which will operate cash dispensers, pay bills by instantly deducting funds from a deposit account or drawing on a line of credit and switch money from one account to another. It will be used in conjunction with a PIN (personal identification number) rather than a signature, which raises a host of legal problems, for under our present system a person's signature, rather than his word, is his bond. Replace that with a number, and we need a new set of rules to ensure that the owner of the number lives up to his financial obligations, that nobody borrows or steals his number, and that the other numbers he deals with perform their part of the bargain.

At present, there are no adequate laws governing the use of credit cards, which have been with us for a decade. Many statutes and rules may apply, but there is a great deal of uncertainty. The need for certainty in this area stems from the need to balance the interests of all parties to credit card transactions with respect to the distribution of unsolicited cards, the apportionment of loss resulting from unauthorized use, the disclosure of terms, the availability of consumer defences vis à vis the card issuers, and the right to chargeback. The transformation of credit cards into transaction cards will require that the uncertainty be cleared up, not just by provisions in contracts but by new laws.

(4.1) *It is recommended, to begin with, that legislation be enacted regarding credit cards. The recommendations of this report regarding transaction cards in a EFT environment should then become additional provisions of this legislation.*

Billing statements will become even more essential than they are now to help the customer keep track of his non-cash, electronic transactions. However, a credit card billing statement -- a "descriptive" billing that lists the goods or services purchased -- may not be accepted as proof of payment. Its value in law is unclear. In contrast a cancelled cheque provides limited proof of payment because the creditor's endorsement on it is an admission against interest that he has received the money and this can be used in litigation. But in EFT there is no cancelled cheque or sales slip -- only electronic impulses on tape or printouts from these impulses. At this point, the records of the financial institution which issued the transaction card would become important in satisfying the question of whether payment has been made. Those records may not be admissible in court under The Ontario Evidence Act (section 35(2)).

So, if transaction cards are to be acceptable to consumers, they must be backed up by written documentation having the validity of a cancelled cheque which can be used to settle disputes over payment.

(4.2) *It is recommended that legislation be enacted requiring documentation of every EFT transaction triggered by a transaction card. This documentation should be available at the time the card is used and it should contain specific information designated by statute. A copy of the information on the sales slip should be provided in the subsequent billing statement.*

Bank and near-bank records provide important evidence in lawsuits -- sufficiently important to require separate treatment under The Ontario Evidence Act. They are becoming even more important as these financial institutions take on the task of recording their customers' deals and the contributions of all parties to a transaction. They are now doing this electronically, making records difficult to get at and costly to retrieve from their computerized systems. If the operator of a system is made to pay the cost of retrieving information for use in legal disputes, he is likely to have the system altered to make retrieval quicker and easier.

(4.3) *It is recommended that consideration be given to amending The Ontario Evidence Act to ensure that the cost of retrieving computer information is borne by the operator of the system. The Act must also be amended to govern the admission of computer information as evidence.*

Errors occur in any system. There are long-established methods of correcting them in the cheque system. With credit cards the situation is unclear. By the agreement he signs when

he takes out a card, the customer takes responsibility for correcting errors other than those caused by the card issuer. And there are no direct statutory provisions to prevent the issuer from dodging all responsibility for error.

EFT transaction cards will probably increase the number of errors, while introducing a new form of error caused by malfunction in the electronic equipment. This will not always be the fault of the financial institution which operates the system, but it should bear the responsibility because (a) it can divide the liability with whoever made the sale, and (b) the consumer should not have to bear a new business risk.

In the credit card system, errors caused by the card issuer can be corrected only if the issuer agrees that an error has been made. Transaction card errors will be even more difficult to resolve because the issuer has all the pertinent information stored in his electronic files. The cardholder must have the statutory right of access to it in any dispute.

At present, the card issuer has the upper hand.

(4.4) *It is recommended that legislation be enacted to ensure an adequate method of error resolution with minimum standards of conduct which prevent any further erosion of the cardholder's power to resolve disputes. This should establish rights to obtain copies of pertinent documents, define time periods for investigations of disputes, provide for the suspension of claims for*

payment while a matter is being investigated, a refund of credit charges on disputed items, and the reversal of entries found to be in error. It should place the responsibility for all system malfunctions upon the card issuer regardless of how the malfunction was caused.

Under the cheque system, the writer of a cheque can stop payment on it in the time (usually up to 24 hours) before it is cleared and the money deducted from his account. This gives him some protection if the goods or services he has purchased with the cheque are not forthcoming or turn out to be faulty. It's only a fleeting protection and by stopping the cheque he may breach his legal obligation to pay, but it is a form of safeguard against unsatisfactory transactions for goods or services. Under the present credit card system, he has no right to stop payment, and with a transaction card activating electronic equipment to make the transaction virtually instantaneous, he won't have time.

So in preparing credit card legislation we should consider whether to include a statutory right for cardholders to stop payment. The EFT equivalent of a stopped payment is a reversal of the transaction, called a "chargeback". The capability to reverse transactions will be built into any EFT system to handle the correction of errors, so there would be no technical difficulty if a chargeback right were established. The argument for this is that the user of a transaction card should have the same ability to stop payment now possessed by the writer of a cheque.

The effect of the right to reverse a transaction or claim a chargeback is to shift the burden of taking legal action from the cardholder to the person who sells him the goods. Many merchants offer "satisfaction or your money back" guarantees which, if actually honoured, are similar to a chargeback.

The creation of a legal right to chargeback would make such promises of adjustments and returns enforceable. There should be a time limit of a few days at the most in which customers can use the right of chargeback and the remedy should apply only to durable, returnable goods of more than a specified dollar price; otherwise, chargebacks would become a burden on the system.

There are two ways of providing chargebacks. One is to delay the actual electronic transfer of funds between cardholder and card acceptor for several days (this is called "value dating"). The other is to process the transaction immediately but allow it to be reversed within a specified period of a few days. The second method appears to be more desirable because "value dating" holds up the whole EFT process and nullifies its principal benefit -- speed.

(4.5) *It is recommended that a statutory right of reversibility be granted to transaction cardholders. This would, as far as possible, be the equivalent of the present stop payment right in the chequing system.*

The concept of "consumer defence" embodied in section 42(a) of The Ontario Consumer Protection Act does not cover either credit card or transaction card matters. It should be extended to do so.

This defence does not exist in common law. If cardholder 'A' is dissatisfied with the goods he bought from merchant 'B' and, as a result, refused to pay his credit card bill to card issuer 'C', then 'C' can sue him for the money and 'A' has no defence because he still owes 'C' the money, regardless of his dispute with 'B'. He has a credit contract with 'C' which is quite separate from his sales contract with 'B'.

The consumer defence concept protects purchasers from unscrupulous merchants who may try to hide their responsibilities behind the legal framework used to provide the financing for the deal. If you buy a car that turns out to be a "lemon", and you financed it, you can hold the financier, as well as the dealer, responsible when he demands payment because he has an interest in the "lemon", even though he was not a party to the sale. But this Act does not cover credit or transaction card purchases.

(4.6) *It is recommended that in EFT transactions a cardholder be entitled to assert the same defences against the card issuer as he would be entitled to assert against the person who accepted the card in completing the sales transaction.*

SECTION FIVE: CONSUMERS' RIGHTS

"Will that be cash, or Chargex?" As these broadcast commercials point out, we now have a choice. (We can also pay bills by cheque.) But for how long? Big financial institutions have ways of coercing their customers into using the system of payment most convenient to them. These can be direct, through stipulating the method of payment before extending credit, or indirect, by offering discounts to consumers or merchants. As EFT systems will be cost-effective only if they are generally used we can expect attempts to force them upon us. Therefore, action is proposed to protect a consumer's right of choice before it comes under attack. And it must be a real protection -- not merely the preservation of the consumer's right to opt out, which is seldom exercised.

(5.1) *It is recommended that the consumer's choice concerning the mode of payment of a debt be protected by statute. Such a provision should prevent the coercion of consumers into receiving their financial services in a particular form. The statutory protection should require an informed consent carrying with it the right of revocation.*

The consumer must know what he is getting into. An EFT transaction card is a complex new tool. The cardholder must be told exactly how it works, its benefits and drawbacks, and what its various services will cost him. The Consumer Protection Act already requires disclosure of interest rates

and other charges in certain situations. This legislation needs to be extended to cover credit and transaction cards. The card-issuer can be expected to explain to the customer how to use the card, since this is in his interest. It is up to the government to make sure the customer is also told of his rights. These rights, as proposed in this report, should include the stopping of payment (chargeback), ways of correcting errors, limitation of liability for loss caused by unauthorized use of the card, and control over the dissemination of information concerning his finances.

(5.2) *It is recommended that existing provincial legislation dealing with disclosure in and advertising for certain types of lending transactions be extended in scope to include transaction cards. These statutory disclosures should be made in clear and meaningful terms at the time of entering into a contract for the transaction card.*

To promote their services, credit card companies mailed out large numbers of cards to people who had not applied for them in the hope that they would be used. Some went astray and were used illegally, causing losses. Provincial law does not prohibit the distribution of unsolicited cards but now places liability for any losses incurred squarely on the distributors. No action can be brought against a person to whom credit was extended through a card unless he requested or accepted the card.

The danger of theft by use of a transaction card is much greater because the card, plus the PIN identification number, can be used for a greater variety of purposes and no signature is required. So, at the very least, the present laws should be extended to cover unsolicited transaction cards. If unsolicited distribution is not to be prohibited entirely, the cards and their identifying PIN numbers must not be sent out at the same time. This will reduce the chance of theft without restricting card-issuers who want to take the risk of marketing in this way.

(5.3) *It is recommended that provincial legislation dealing with unsolicited credit cards be extended in scope to include transaction cards within their provisions. The legislation should also be expanded to prohibit the simultaneous distribution of a transaction card and its unique identifier and make liability for unauthorized use of an unsolicited card entirely that of the issuer.*

Present credit card contracts generally stipulate that the cardholder pay the first $50.00 of sums lost through unauthorized use of his card. The issuer absorbs the rest. The incentive to notify the issuer of loss of the card lies in the notice being received before any unauthorized use occurs -- thus saving the cardholder's first $50.00 of monies lost. With transaction cards, theft will be quicker and easier. Once the thief has got hold of a card and the PIN number to go with it, he can obtain money in seconds. He does not have to forge

a signature or face a human clerk. Therefore, transaction cards reduce the likelihood of the notice of loss being received before any unauthorized use occurs. The incentive to report the loss of his card in order to save the $50.00 of liability is gone.

New policy on liability will be needed to cope with the age of transaction cards. The key to responsibility for loss is the PIN number. Under the credit card system merchants must verify the cardholder's signature before allowing a transaction to go through. When signatures are replaced by PIN numbers it becomes the cardholder's responsibility to guard his number. He has control of the method of verification.

If he is careless with it, by keeping it attached to his card so that both tools can be stolen at once, or voluntarily gives away card and number, he must bear the loss. In every other situation the card-issuer should bear the loss because, as stated, the $50.00 limit is unrealistic. Therefore, a new balance of liabilities should be struck.

(5.4) *It is recommended that legislation be enacted concerning liability for unauthorized use of a transaction card. The only time the cardholder should be liable would be for failure to notify the card-issuer of loss of the card or if he facilitated the unauthorized use by keeping the transaction card and PIN number together or voluntarily gave them to someone. The legislation will have to permit the recredit of unauthorized transactions.*

Transaction cards and other EFT services will be offered only to people with accounts at banks or near-banks. This excludes low income consumers and people with marginal credit ratings who do not have accounts. If transaction cards are to provide cheap and convenient financial services, a way must be found to allow low income consumers to share the benefits. Financial institutions are unlikely to invite them to use EFT unless they are given incentives to take the necessary financial risks.

(5.5) *It is recommended that a joint industry-government committee be struck to devise a system of incentives to ensure that the benefits of EFT to low income consumers can be provided on a basis satisfactory to all.*

TO SUMMARIZE SECTIONS FOUR AND FIVE:

A transaction card system will make and record transactions electronically but provide written statements of accounts. It will verify balances and, where necessary, detect and rectify errors. The mode of operation will be determined and disclosed in the initial agreement between card-issuer and cardholder establishing a transaction card account. This will be a crucial document, aspects of which require statutory control. Legislation is required to protect cardholders from unfair practices and to ensure that documentation of transactions can be used in court evidence. Such a legal framework, established before EFT becomes more widespread, will provide the fundamental principles needed to cope with this dramatic change in our ways of handling money.

In the next section the responsibilities of the Province of Ontario in providing this framework are discussed.

SECTION SIX: WHO WILL LEGISLATE?

From the legal aspect, there are two ways of looking at EFT:

It is a means of transferring money into and out of banks and other financial institutions, using telecommunications -- and both banking and telecommunications come under federal jurisdiction.

But it also affects the individual's concern for privacy and his contractual relationships, which are provincial matters under our present constitution, coming under the heading of "property and civil rights within the Province".

The second view is no less legitimate than the first. So the Province of Ontario can, up to a point, set rules which will shape the environment in which EFT systems are developed and marketed. The federal government has taken no action. Yet, as this report indicates, the need for control is urgent. The Province should exercise its untapped constitutional authority.

The two major limiting factors on provincial authority are the scope of federal powers and the format in which provincial control is enacted. The extent of the federal powers is unclear at the moment but is probably not nearly so broad as is generally assumed. This report recommends that new legislation be enacted and that existing legislation be amended.

Careful attention to drafting technique with application to all financial institutions will assure the province's power to enact such legislation.

The federal jurisdictional fields of banking and telecommunications have not been carefully circumscribed by the courts. Nor have they been consistently broadly interpreted. The traditional interpretation of the British North America Act is that if a matter does not fall squarely within the federal field, all its local, private and intra-provincial aspects will fall within the provincial domain and be immune from federal interference.

Despite the assumptions of some federal advisors, it seems reasonably clear that this form of interpretation applies to the powers of banking and telecommunications. So provincial contract laws with broad application could govern private transactions, notwithstanding the fact that one of the contracting parties is a federally-chartered bank. Similarly, provincial privacy legislation would apply, within the Province, notwithstanding the fact that the information involved may be stored in a nation-wide computerized network.

As financial institutions appear to be developing their EFT systems in competition with one another and also decentralizing their operations, some of them may be conducted entirely within the province, separate from nation-wide "banking" and inter-provincial telecommunications and wholly within provincial control.

Ontario has the power to "make laws in relation to . . . Civil Rights in the Province". It can protect existing civil rights and create new ones. The ones which are clearly within provincial control and basic to supervision of EFT developments are the rights to consumer protection, Sale of Goods Act remedies, propriety rights, and protection of contractual obligations.

EFT will cause legal problems related to provincial civil rights. These include the problems of introducing evidence of transactions recorded electronically, privacy and confidentiality of information stored in, and transmitted by, electronic systems, and protecting the rights of the user in transaction card matters.

The power of the province to regulate the admission of evidence in its courts, is clear. Privacy is a concept, not a civil right. Federal law protects us against wire-tappers and Peeping Toms as a matter of criminal law, but does not provide any civil procedure to preserve privacy. This is the job of the province.

It is up to the province to preserve and defend these rights against invasion by federally-supervised banks, by near-banks, or by telecommunications networks. If and when the federal government decides to defend them too, there may be overlapping legislation, but we have this already in, for example, dangerous (federal) and careless (provincial) driving charges. Dual protection is better than no protection at all.

There is a woeful lack of legislation, federal or provincial, covering the use of credit cards and none to cover transaction cards. However, credit card contracts, as they affect civil obligations within the province would appear to be subject to provincial legislation and transaction card contracts are an extension of these. Such provincial legislation could co-exist with federal laws unless the federal Parliament attempts to take over the entire field itself. As Parliament shows little sign of doing this, there is not only room for provincial legislation, there is an urgent need for it.

SECTION SEVEN: WHAT NEXT?

Science and technology, with business hot on their heels, generally outrun legislation. This report attempts to catch up with scientific and technological advances that have already occurred and propose legal answers to the problems they may cause as they are put to use. As was stated at the outset, this is not the definitive Canadian report on EFT, only the first one, and it should be built upon and updated.

Looking further ahead, there are more EFT problems that do not need to be dealt with immediately but bear watching. But two of these future problems are the POS (point of sale) terminal and the ACH (automatic clearing house).

EFT systems are expensive. In the United States, which has more and smaller banks and near-banks than does Canada, and where financial power is not so concentrated, these institutions are co-operating and sharing resources in order to pay for EFT systems. For an American, this raises the threat of monopoly, Big Finance crushing competition and squeezing the "little guy" out. In Canada, where we are used to a few large banks, pooling of resources may even preserve the spirit of competition, by allowing the near-banks to compete with the banks. But ultimately the storekeepers, the front line troops in the EFT armies, may demand one giant EFT system, rather than several large competitors, to save them money. They may install POS (point of sale) terminals which will be shared by all systems.

Such action is the potential forerunner of a one-system, nation-wide or even continent-wide financial operation.

Shared or not, the emergence of POS terminals and other developments will probably spawn the creation of automated clearing houses (ACH) which may be shared by several if not all of the EFT systems. This electronic counting house will automatically process taped transactions, sort the data according to the receiving depository institutions, prepare aggregate accounting information for debit and credit to the appropriate depository institution, and distribute this information to the various institutions for the purpose of settlement of accounts.

Such developments could cause EFT systems to grow dramatically, perhaps to the extent where they will outgrow the controls proposed in this report. And no doubt there are other technological advances in the works that we do not know about yet.

So, in conclusion, it is urged that the Province of Ontario not only keep an eye on further developments in EFT but be ready to respond to them.

(7.1) *It is recommended that the Province of Ontario continue to monitor EFT developments to ensure that they do not outrun this or any other studies it may undertake. This monitoring should identify new issues as they arise and encourage public debate on what new legislation, if any, may be required.*

SECTION EIGHT: SUMMARY OF WORKING PAPER RECOMMENDATIONS

The content and recommendations of this report were drawn from the background working papers comprising the research project. This section repeats, under their various section headings, the report recommendations. Below each recommendation are its supporting working paper recommendations with cross references to the papers.

Section Three: Privacy in Danger

(3.1) *It is recommended that Ontario enact a statutory right to financial privacy. This legislation would establish who has the right of access to financial data and limit the use of disclosed information to such authorized persons. These persons would be permitted to use the data only for the purposes for which access was granted. Failure to observe such standards would give rise to statutory rights to damages against the financial institution concerned. This legislation could be part of a broader piece of legislation dealing with privacy.*

1. Consider the enactment of a statutory right to financial privacy along the lines of the California, Illinois, and Maryland models, which would mandate confidentiality for financial transaction information, control third party access to customer data, require notice to customers of requests for access by third parties, limit the scope of data collection, and establish statutory minimum damages

at a significant dollar amount for breach of duty by unauthorized disclosure of personal financial data. (Working Paper (W.P.) #5 Recommendation (RECM.) GOV'T. #4.)

2. Reinforce the existing implied contract between financial institutions and customers/depositors by a statutory provision to prohibit contracting out of information rights and to design proper releases for individuals to sign when entering into financial relations with financial institutions. (W.P. #5 RECM. GOV'T. #5.)

3. Grant customers of financial institutions a property interest in their financial transaction information. (W.P. #5 RECM. GOV'T. #6.)

(3.2) *It is recommended further that financial institutions improve their methods of handling personal information relating to their customers to ensure the highest standards of confidentiality. The government should monitor their progress and, if self-regulation fails, enact legislation to protect the confidentiality of customer data and information about financial transactions by setting rules for proper employee conduct.*

1. Publicly affirm and maintain the highest standards of confidentiality for customer data and financial transaction information. (W.P. #5 RECM. INSTIT. #1.)

2. Draw up and implement basic rules and regulations for the collection, protection, and disclosure of personal information and financial transaction data. (W.P. #5 RECM. INSTIT. #2.)

3. Draw up and implement voluntary industry guidelines for the confidentiality and security of customer data and financial transaction information. The Directors of a financial institution should require their internal audit department to certify that their institution is in compliance with the guidelines. (W.P. #5 RECM. INSTIT. #3.)

(3.3) *It is recommended that an industry-government committee be established to draw up guidelines for the confidentiality and security of customer data and financial transaction information. These should include measures to restrict unauthorized access to data by employees of financial institutions, division of responsibilities among employees, and monitoring of the systems. Special training programs for employees should be established.*

1. Implement measures to restrict unauthorized access to customer data and financial transaction information by employees of financial institutions, including training programs and monitoring. (W.P. #5 RECM. INSTIT. #4.)

2. Continue to monitor the development of EFT systems in Canada in order to protect the interests of citizens in the privacy, confidentiality, and security of their personal data. (W.P. #5 RECM. GOV'T. #2.)

3. Promote the preparation of voluntary guidelines, standards and regulations for the protection of confidentiality in the operation of personal data systems in the financial field. The model guidelines prepared by the Privacy Committee of New South Wales in April, 1977 are exemplary in this connection. (W.P. #5 RECM. GOV'T. #3.)

Section Four: Paying by Numbers

(4.1) *It is recommended, to begin with, that legislation be enacted regarding credit cards. The recommendations of this report regarding transaction cards in a EFT environment should then become additional provisions of this legislation.*

1. The relationship between the consumer, card issuer and merchant involved in a credit card transaction is created in part by contract. The result is a hybrid commercial device that has some characteristics of many of its better understood predecessors. This state of affairs, means that while many statutes and common law rules <u>may</u> apply to credit card transactions, it is totally unclear which rules do in fact apply. It is largely a question of characterization, an observation which helps very little. The need for certainty in this area stems from the need to balance the interests of all participants. The urgency of this need will not abate with the spread of electronic payments, but will

increase. Therefore, it is urged that the province consider legislation which would provide legal certainty by defining the rights and obligations of all parties to credit card transactions with respect to, inter alia; the distribution of unsolicited cards, the apportionment of loss resulting from unauthorized use, the disclosure of terms, the availability of consumer defences vis à vis the banks and the right to chargeback. (W.P. #8 RECM. #1.)

(4.2) *It is recommended that legislation be enacted requiring documentation of every EFT transaction triggered by a transaction card. This documentation should be available at the time the card is used and contain specific information designated by statute. A copy of the information on the sales slip should be provided in the subsequent billing statement.*

1. The cheque, endorsed by the payee represents a major element of proof in contemporary payments litigation. The obsolescence of the cheque in the electronic age will make some form of equivalent essential. It is submitted that legislation requiring the delivery of documentary evidence of every EFT transaction to the consumer involved should be seriously considered as a solution to this problem. If such documentation is mandated, consideration should also be given to making it prima facie proof of the transaction recorded. (W.P. #7 RECM. #10.)

2. When a consumer has effected a non-cash transaction, he depends in part on others to complete the transaction for him. For example, when writing a cheque or signing a sales draft the consumer relies on the bank to debit the correct amount from his account and pay it to the proper payee. Since these functions are beyond the immediate control of the consumer he must, to avoid error, verify transactions after the fact by reviewing cancelled cheques and credit card billing statements. Cancelled cheques serve not only to satisfy debtors that the proper payments have been made but as well to prove payment to a doubting creditor. The value of descriptive billing statements as proof of payment remains unclear at present, but they at least allow debtors to monitor their credit card accounts. These two facets of cheques and credit cards must be preserved in an EFT environment if it is to be acceptable to consumers and workable from a dispute settlement point of view. To ensure this objective it is recommended that consideration be given to statutorily requiring documentation of every EFT transaction, stipulating the contents of such documentation and providing for the evidentiary efficacy of such records. Likewise, consideration should be given to mandating the contents of descriptive billing statements to insure their utility. (W.P. #8 RECM. #5.)

(4.3) *It is recommended that consideration be given to amending the Evidence Act to ensure that the cost of retrieving computer information is borne by the operator of the system. The Act must also be amended to govern the admission of computer information as evidence.*

1. The admissibility of electronic records must be established and preserved if the litigation process is to continue to function as a system for payments dispute resolution. To this end, the judicial interpretations of the business records provisions of the Canada and Ontario Evidence Acts and the Common Law, in particular section 36 of The Ontario Evidence Act and Rules 326-352, must be monitored. If it is determined that the constructions being placed on the current law are not flexible enough to accommodate innovations in record keeping, then the admissibility of electronic payments records must be ensured by amendments to section 36 of The Ontario Evidence Act. While the statutes with evidentiary provisions relating to "documents" and "records" are of particular significance, all provincial statutes referring to those terms must be reviewed in order to determine whether they accommodate electronic records or printouts. If they do not, either expressly or as a result of judicial interpretation, they should be so amended. (W.P. #7 RECM. #1.)

2. The word "record" is the key to the admissibility of electronic business and bank records. The Ontario Evidence Act states in section 36(1)b, that "record includes any information that is recorded or stored by means of any device." The Canada Evidence Act states "record includes the whole or any part of any book, document, paper, card, tape or other thing on or in which information is written, recorded, stored or reproduced, and, except for the purposes of subsections (3) and (4), any copy or transcript received in evidence under these sections pursuant to subsections (3) or (4)." Although both these provisions are admirably broad in scope, they focus on a different concept of "record" in each case. The provincial statute equates record with information. The federal statute suggests that records are the tangibles on or in which information is stored. [This variation of approach highlights one of the many questions surrounding the records issue which flow from the fundamental fact that electronic records are imperceptible to the human senses. Only when they are printed out or otherwise displayed can they be read.] The "record" could be the stored electronic impulses, it could be the transformation of that record, the printout, or it could merely be the information.

In addition to the basic problem of admissibility referred to in recommendation 2, this range of possibilities

raises another significant problem because of the principle of law which states that documents produced for the purpose of litigation are privileged and need not be produced for discovery. If the "record" is the printout then it could be privileged as in many cases no printout of the electronic record is made in the ordinary course of business. If, on the other hand, the record is by definition, made when the electronic impulses are created by input to the computer in the ordinary course of business, there can be no suggestion that the record is made for the purpose of litigation, and no question of privilege can exist. Insofar as full disclosure and discovery are essential aspects of civil litigation it is desirable that such procedures be preserved. Accordingly, if it is determined that the records referred to in the current laws are the print-outs, they will have to be excluded from classification as privileged by statute if this is not accomplished judicially. (W.P. #7 RECM. #5.)

3. Bank records now form an important part of the evidence tendered in payments cases. In recognition of this, such "documents" receive special attention in the Evidence Acts. As the conversion to EFT progresses the number of electronic transactions handled and recorded by banks will increase. Accordingly, the judicial interpretations of the bank records provisions in section 34 of The

Ontario Evidence Act must be monitored. Again, as in the case of business records, if the development of the case law is unsatisfactory, legislative action must be taken to redefine "record" within the meaning of the Act so as to include electronic records of every conceivable type. As a final note on the subject of section 34, serious consideration should be given to expanding the scope of the section by making it apply to all financial institutions instead of only chartered banks. This could be accomplished by changing the definition of "bank" in the section. (W.P. #7 RECM. #2.)

4. The admissibility of electronic records under the Evidence Acts is of vital importance because documents generally speaking are hearsay. A computer-generated document, qua document, is therefore hearsay. Moreover, a computer generated document may be double hearsay in that the machine may only be repeating information that it was told, either by a human input operator at a keyboard or another computer or a machine such as an automatic teller machine. If one thinks of the customer at the automatic teller machine putting data into the system, the output becomes triple hearsay.

Section 36(4) of The Ontario Evidence Act circumvents this problem as it purports to make hearsay statements in business records admissible. Section 30(1) of the Canada Evidence Act on the other hand makes business

records admissible only where oral evidence in respect of the same matter would be admissible. This suggests that only documents which record the personal knowledge of the maker may be admissible. The cases on the Canada Evidence Act to date do not assist in the resolution of this apparent conflict. Given that there are some matters to which both Acts may apply, this inconsistency represents a serious threat to commercial and legal certainty. The cases on both statutes must be monitored and if the conflict is not therein resolved, remedial legislation will be necessary. (W.P. #7 RECM. #6.)

5. The cost of retrieving electronic records for inspection, production and discovery, and for use in evidence at trial can be very considerable and could well exceed the amount of money in dispute. Such costs must be allocated to either the plaintiff, defendant, or electronic record keeper. Rules 347, 348 and 349 govern the production and inspection of documents. Rule 326 governs examination for discovery. Amendments adding cost allocation provisions to these rules should be considered. (W.P. #7 RECM. #3.)

6. In connection with the question of record retrieval costs, section 34(6) of The Evidence Act currently gives a judge discretion to order that the cost of bank record inspection be paid by the bank where such costs have been occasioned by default or delay on the part of the bank.

Consideration should be given to deleting the requirements of default or delay in this statute so that the social cost of electronic record keeping is borne by those responsible for its evolution. (W.P. #7 RECM. #4.)

7. Consideration should be given to whether a statutory standard of computer evidence reliability is to be imposed (as in England) or whether the veracity, accuracy, and credibility of computer "evidence" is to be tested in the traditional method of cross-examination. (W.P. #7 RECM. #7.)

8. Recommendation number 7 (the one above) deals with the problem of computer evidence at trial, however, the problem of the accuracy, and veracity of computer output will present itself before trial, at the stage of production and discovery. In the future, an affidavit on production pursuant to Rule 347 will undoubtedly refer to computer documents and the operation of the party's computer will be an area for examination on discovery pursuant to Rule 326. Parties will wish to know whether such documents are accurate, whether all relevant documents have been generated and produced and how the computer output was generated. To this end they may wish to assess their opponents data processing equipment and run verifying programs. Such a procedure could conceivably be within the scope of the experiments

contemplated in Rule 372. The cases on this Rule should be monitored, and if litigants employ this procedure some attempt to regulate it should be made because of the cost and privacy implications inherent therein. (W.P. #7 RECM. #8.)

9. There was a time when witnesses were allowed to testify only as to their personal knowledge; they were not permitted to offer their opinions. Latterly, however, expert witnesses have been permitted to give opinions on matters relevant to the lis. The testimony of a medical doctor as to the cause of a particular complaint afflicting a party is a typical example; another is the police radar operator giving evidence of the speed of a vehicle based upon the readings on a radar device. The potential exists for the circumvention of the problems of admissibility surrounding computer records by the use of an expert witness. Such a witness could give his opinion on, for example, the status of an EFT account based on a printout, and his expertise. In the United States, even in cases where it has been sought to adduce computer evidence as business records, the practice in some cases has been to call such a huge volume of evidence to support its accuracy that days of court time and much of the trial is so taken up. If experts were to give opinions based on computer output, similar practices would likely develop to support their opinions. With a view to regulating the volume of

supportive evidence necessary in such cases, and therefore costs, consideration should again be given to the adoption of a statutory standard of proving computer reliability and hence admissibility. (W.P. #7 RECM. #9.)

10. The concept of negative proof is dealt with in section 30(2) of the Canada Evidence Act. Much payment litigation flows from non-payment and, the absence of a record of payment in a record is an important piece of evidence of non-payment. As the computerization of business records spreads, the possibility that the absence of a computer record of payment will be the only evidence of non-payment increases, and the importance of negative proof increases accordingly. The Ontario Evidence Act does not have a negative proof provision and for the reasons expressed above, the Ontario law should be reviewed and stated in the Evidence Act. (W.P. #7 RECM. #11.)

(4.4) *It is recommended that legislation be enacted to ensure an adequate method of error resolution with minimum standards of conduct which prevent any further erosion of the cardholder's power to resolve disputes. This should establish rights to obtain copies of pertinent documents, define time periods for investigations of disputes, provide for the suspension of claims for payment while a matter is being investigated, a refund of credit charges on disputed items, and the reversal*

of entries found to be in error. It should place the responsibility for all system malfunctions upon the card issuer regardless of how the malfunction was caused.

1. This recommendation recognizes that errors are an inevitable part of transactions involving payment and suggests measures which would assist in their detection. There must also be a method of error correction. Current payments errors are resolved by reference to a body of law which has an undetermined relevance to credit card transactions. Thus, error resolution in that scheme and in future EFT systems is largely an unknown quantity. It seems likely however that as the number of EFT participants increases, the number of errors will also increase, and that a new species of error, the systems malfunction error, will evolve. An allied problem is the question of where the burden of error induced losses must fall. An observable tendency in response to these uncertainties has been that of card issuers shifting responsibility away from themselves, at the expense of the cardholders. Not all systems errors will be the fault of the financial institution. Some will undoubtedly be traceable to communications suppliers. Even so it is recommended that the financial institutions bear this responsibility because they can divide liability with their suppliers. Otherwise another business risk will be shifted to the consumer. To prevent further erosion of the cardholder's

position and to insure an adequate method for error resolution and loss placement, it is recommended that minimum standards of conduct in that regard be enacted. For this purpose, Senator Riegle's EFT bill is a model worthy of examination. (W.P. #8 RECM. #6.)

(4.5) *It is recommended that a statutory right of reversibility be granted to transaction cardholders. This would, as far as possible, be the equivalent of the present stop payment right in the chequing system.*

1. When a consumer pays for merchandise with a cheque he can countermand the cheque before it is paid by his bank. This right exists only between the bank and its customer and does not affect the relationship between the merchant (payee) and the customer (payer) in any way. The customer still owes the merchant the price of the goods and if the customer in fact had no legal right to refuse payment, then by stopping the cheque the customer breaches the sales contract and will be liable for the price of the goods and possibly even damages. The stop payment merely shifts the burden of suit to the merchant in situations where the customer seeks to avoid a sales contract because of defects in the goods sold. In a credit card system governed by the cardholder/card issuer contract there is no such stop payment right because none is granted. In a real time EFT system stop payments are impossible because the transaction is

completed instantaneously, the parallel right would be to reverse the payment transaction. Again neither of these exercises affect the obligations under the sale contract. With the disappearance of the cheque, the stop payment right now enjoyed by consumers will also vanish unless a similar right of chargeback is statutorily created. It is recommended that this be done, but it is to be emphasized that a mere replication of the stop payment rights associated with the cheque system is not advocated. The new right should apply to sales of goods and services, the value of which is above a fixed dollar amount to prevent unnecessary expense and should only be available where the consumer has a legal right to resist payment of the contract price. The right to effect chargebacks must also carry the obligation to return the goods over which the payment dispute arose. A final condition precedent to the availability of the chargeback right should be the requirement of bona fide attempts to resolve the dispute between the merchant and the consumer. (W.P. #8 RECM. #8.)

(4.6) *It is recommended that in EFT transactions a cardholder be entitled to assert the same defences against the card issuer as he would be entitled to assert against the person who accepted the card in completing the sales transaction.*

1. The concept of a consumer defence refers to those defences which are asserted against financial intermediaries associated with consumer transactions. In the past, unscrupulous merchants effectively isolated themselves from consumer complaints regarding defective goods by assigning conditional sales contracts to third party financiers who would give the merchant the value of the goods but who were not subject to the equities between the customer and merchant. The consumer always had a right of action for damages against the merchant, but the burden of suit to recover the damages was sufficient to inhibit most such actions. Section 42(a) of the Consumer Protection Act (CPA) now protects consumers from these practices by preserving their right to assert defences flowing from defective merchandise against the financiers. When card issuers extend credit to cardholders, they act as financiers but may be immune to consumer defences. This is so because section 42(a) of the CPA may not apply to the card issuers because of the definitions contained in that Act. As the volume of credit card transactions increase and card issuers abandon their market strategy of not enforcing their strict legal rights against cardholders, the importance of whether section 42(a) is applicable to card transactions will escalate. It is recommended therefore that legislation similar to section 42(a) of the CPA but with applicability to transaction cards be enacted to prevent the isolation of

card issuers from the defences of the cardholders. Such a statute should be complimentary to the chargeback enactments recommended above, and should provide for similar limits on the availability of the consumer defences. That is to say, the existence of the defences should be dependent on prior negotiations and be limited to transactions above a fixed dollar limit. (W.P. #8 RECM. #9.)

Section Five: Consumers' Rights

(5.1) *It is recommended that the consumer's choice concerning the mode of payment of a debt be protected by statute. Such a provision should prevent the coercion of consumers into receiving their financial services in a particular form. The statutory protection should require an informed consent carrying with it the right of revocation.*

1. At the present time consumers enjoy a choice when it comes to the mode of payment of a debt. Cash, cheques and credit cards are the main alternatives. For reasons of economy of scale, among others, some creditors prefer one mode of payment over others. Large creditors like chartered banks have the power to coerce consumers into using one mode or another. The means may be direct, as in a contract of adhesion, or indirect as in the case of discounts either to consumers or merchants. Universality of use is a key to making EFT systems cost-effective and therefore the

temptation to use economic coercion on the consuming public will be great. Such a possibility must be prohibited to ensure the continuity of consumer choice in the field of the delivery of financial services. (W.P. #8 RECM. #3.)

(5.2) *It is recommended that existing provincial legislation dealing with disclosure in and advertising for certain types of lending transactions be extended in scope to include transaction cards. These statutory disclosures should be made in clear and meaningful terms at the time of entering into a contract for the transaction card.*

1. In particular, consideration should be given to the following:

(a) Modification of sections 36 and 41 of the Consumer Protection Act (CPA) so that it requires, at reasonable times and in advertising, the disclosure of the cost of borrowing associated with credit and transaction cards.

(b) Amendment of section 37 of the CPA so as to include all card issuers within the definition of "lender" and thereby require rate disclosures at the time of establishing a credit card or transaction card account.

(c) Amendment of section 42 of the CPA so that cardholder defences arising from the transaction with the merchant may be asserted against the card issuer.

(d) The statutory enactment of limited liability for unauthorized use.

(e) The prohibition of unsolicited transaction cards.

(f) The requirement of general disclosure of all terms and conditions applicable to the relationship, including costs, loss shifting clauses, error correction procedures, customer rights and the debit credit switchover.

(g) The prohibition of liability until notice clauses in credit and transaction card contracts. (W.P. #8 RECM. #2.)

(5.3) *It is recommended that provincial legislation dealing with unsolicited credit cards be extended in scope to include transaction cards within their provisions. The legislation should also be expanded to prohibit the simultaneous distribution of a transaction card and its unique identifier and make liability for unauthorized use of an unsolicited card entirely that of the issuer.*

(5.4) *It is recommended that legislation be enacted concerning liability for unauthorized use of a transaction card. The only time the cardholder should be liable would be for failure to notify the card issuer of loss of the card or if he facilitated the unauthorized use by keeping the transaction card and PIN number together or voluntarily gave them to someone. The legislation will have to permit the re-credit of unauthorized transactions.*

1. The problem of the unauthorized use of credit cards takes on an added dimension in an EFT environment. In the present cheque and credit card systems the user is identified, in theory at least, by his signature, and in fact, some transactions in each system are aborted on the basis of an irregular signature. In an EFT system it is likely that identification will be based on a personal identification number known as a PIN number. As a result, anyone with a transaction card and the PIN number will have the appearance of authenticity. This fact changes the locus of responsibility for preventing unauthorized use, from the card issuer and merchants who must verify signatures, to the cardholder, who must keep the PIN number secure. The unauthorized use issue reduces to whether the cardholder should be responsible for some or all of the loss resulting from his careless handling of a PIN number or whether the financial institution which established the system should be. Placing too much of the risk on the cardholder may adversely affect acceptance of EFT systems while the converse may result in cardholder carelessness and large losses. It is recommended that statutory measures be taken to exempt cardholders from liability for unauthorized use except when he substantially contributes to the loss by keeping his card and PIN number together. To make this exemption meaningful, the statute must also provide for the re-credit of unauthorized transactions on notice from the cardholder except in cases of fraud. (W.P. #8 RECM. #7.)

(5.5) *It is recommended that a joint industry-government committee be struck to devise a system of incentives to ensure that the benefits of EFT to low income consumers can be provided on a basis satisfactory to all.*

1. A corollary of the principle that consumers' choice must be preserved is the principle that low income consumers must not be denied access to EFT systems which could provide financial services at rates lower than this segment of the population now pays. As servicing this group is a high risk venture, it is not anticipated that the desired result would be achieved without government intervention. It is recommended therefore that the government co-operate with card issuers in providing financial inducements to insure low income access to EFTS. (W.P. #8 RECM. #4.)

Section Seven: What Next?

(7.1) *It is recommended that the Province of Ontario continue to monitor EFT developments to ensure that they do not outrun this or any other studies it may undertake. This monitoring should identify new issues as they arise and encourage public debate on what new legislation, if any, may be required.*

1. The development, establishment and marketing of EFT services is an expensive enterprise. In the United States, where financial institutions' resources are less concentrated than they are in Canada, this fact has

resulted in co-operation between financial institutions as a means of reducing the investment risk associated with this innovation. The term sharing refers generally to the co-operative establishment and use of EFT hardware and software. An EFT capacity represents a competitive advantage for a financial institution and this fact, coupled with the aforementioned co-operation, raises the spectre of unfair competition by illegal combination and monopoly in all its varied forms. In the U.S. finance industry, the major implication of unfair competition would be the elimination of smaller institutions which could neither join in the system nor compete with it. In Canada on the other hand co-operative EFT ventures may be the only way that the near-banks can continue to compete with the chartered banks.

The consumer also has an interest in sharing as it represents a factor in the ultimate cost and convenience of financial services. The ultimate impetus toward sharing will likely come from retailers who will wish to have one EFT facility to attract business, but not a multitude of expensive terminals and systems. The economics of scale also militate toward having the largest number of participants and this of itself implies sharing of a system, which if it is not universal, should at least be standardized. The sharing issue is complex and far reaching, it has implications which go

to the very heart of the Canadian economic structure. Yet, there has been little debate on the subject and, as a result, an information base from which to develop policy is lacking. It is recommended therefore that developments in the sharing field be monitored so that interest groups and issues can be identified and defined with a view to the ultimate development of criteria for policy determination. In compiling such data consideration should be given to the primary questions of whether sharing should be mandatory or permissive, who should share, what should be shared and at what cost. (W.P. #8 RECM. #10.)

APPENDIX

Working Papers

Working Paper #1
Research Proposal -- Policy and Legislative Responses to Electronic Funds Transfer
Richard H. McLaren, Project Director

Working Paper #2
Canadian Payments System
Richard H. McLaren, Project Director

Working Paper #3
Canadian Banking Techniques
Richard H. McLaren, Project Director

Working Paper #4
Electronic Funds Transfer Technology -- A Canadian Perspective
S. Paula Mitchell

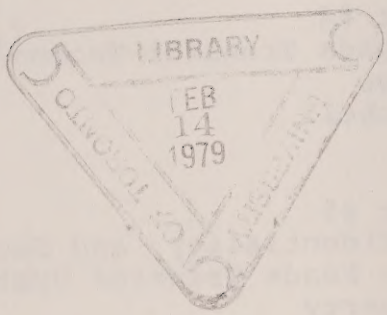
Working Paper #5
Privacy, Confidentiality, and Security in a Canadian Electronic Funds Transfer System
David H. Flaherty

Working Paper #6
Electronic Funds Transfer and The British North America Act -- A Study of the Constitutional Allocation of Legislative Power in Relation to Electronic Funds Transfer Developments in Canada
B. Welling

Working Paper #7
Proof of Payment and Evidentiary Problems -- A Comparison of today's payment system to the computer payment system of the future
A. W. Bryant

Working Paper #8
Transaction Cards in Canada
Richard H. McLaren, Project Director

Methodology Report -- The Methods of Research for "Policy and Legislative Responses to Electronic Funds Transfer"


LIBRARY
FEB
14
1979